INSIDER PRO

EXPERT INSIGHT INTO HOW TECHNOLOGY DRIVES BUSINESS

INSIDER EXCLUSIVE

Way before IoT became a buzzword, industrial verticals had connected systems – now, **NETWORKING INDUSTRIAL DEVICES TO ENTERPRISE IT IS UNLOCKING GREAT POTENTIAL, AND BIG OBSTACLES**

INSIDE INDUSTRIAL IoT:

The **Promises** and the **Challenges**

IDGInsiderPro.com

POWERED BY CIO COMPUTERWORLD CSO InfoWorld NETWORKWORLD

SENSORS ON FACTORY FLOORS AND CONNECTION among all sorts of manufacturing equipment were around for decades before the recent rise of IoT, where disparate, everyday items like thermostats, washing machines and even cars are being hooked up to the internet and probed for valuable data.

Networked industrial devices were called connected systems but were essentially isolated from the world of enterprise IT. IoT is changing that.

The industrial internet of things, IIoT, is a branch of IoT that involves connecting devices and machinery in the energy, transport and other industrial sectors to systems and applications for monitoring, control and data analysis. It involves the merger of classic enterprise IT with operational technology, or OT — essentially, the instrumentation of physical devices and processes.

IIoT promises great productivity gains

IIoT systems allow companies to, among other things, automate, monitor and control machines, vehicles and production processes; track items in supply chains; and collect, store and analyze data for predictive maintenance and inventory management. In this way, IIoT can lead to cost optimization, greater companywide efficiencies and new services for customers.

INTRO

IIoT has also helped spark the creation of complementary technology and concepts such as digital twins, replicas of physical devices that can be used for prototyping and simulating the activity of machines before they are deployed.

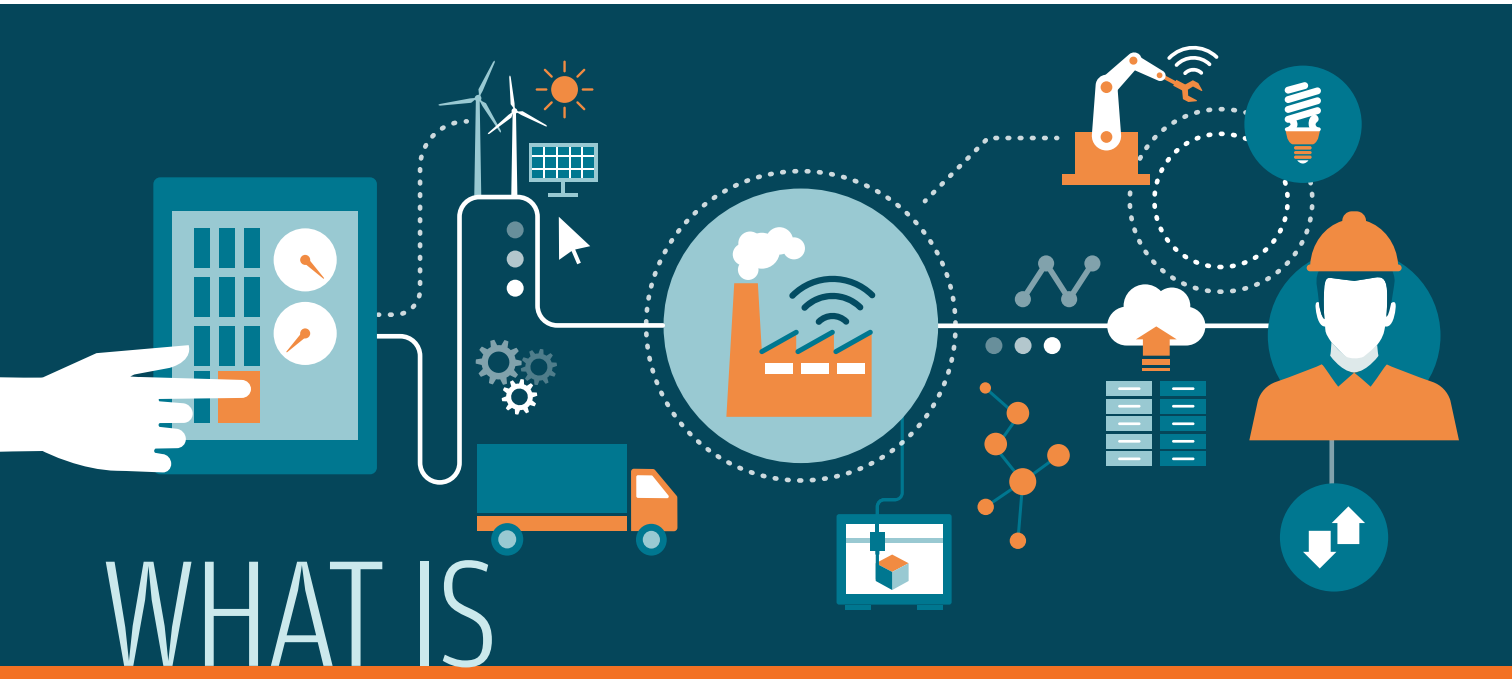
Along with great promise, IIoT poses great challenges. To cite just one complication, there are a wide variety of different networking technologies and protocols involved in machine-to machine communications.

In addition, because IIoT involves critical transportation, industrial and utilities infrastructure, system failure or a crippling attack by hackers could likely be much more serious, and even life-threatening, than hacking consumer items.

Ultimately, IIoT initiatives are too complex to be attempted unless well-defined, overarching business purposes are driving them and shaping their architecture. To accomplish this, staff from the OT and IT side of the house need to come together to shape strategy.

INSIDE

COVER ART: ISTOCK / GETTY IMAGES PLUS / METAMORWORKS



WHAT IS INDUSTRIAL IoT?

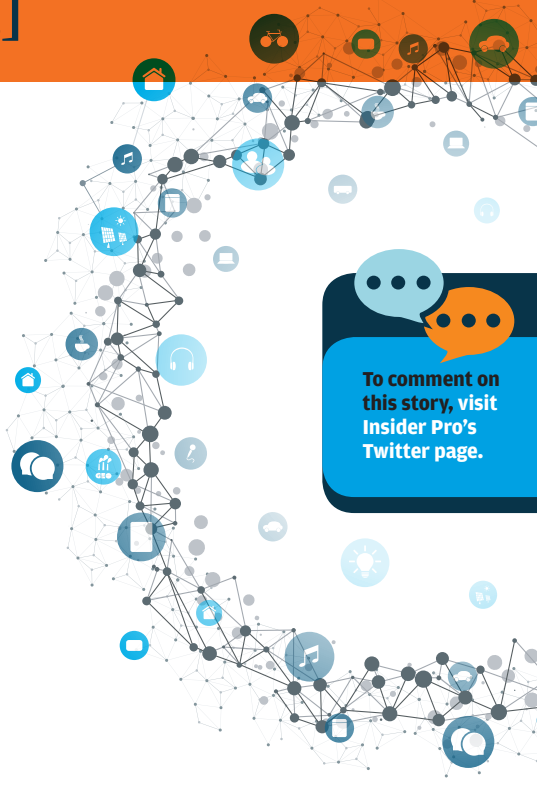
[And why the stakes are so high]

THE INDUSTRIAL INTERNET OF THINGS, or IIoT, connects machines and devices in industries such as transportation, power generation, and healthcare. **The potential is high and so are the risks.** BY JON GOLD

EVERYONE'S HEARD OF THE INTERNET OF THINGS — smart thermostats, internet-connected refrigerators, connected lightbulbs — but there's a subset called industrial IoT that has a much more significant day-to-day impact on businesses, safety and even lives.

What is IIoT?

The term IIoT refers to the industrial internet of things. In broad strokes, it's the application of instrumentation and connected sensors and other devices to machinery and vehicles in the transport, energy and industrial sectors.



To comment on this story, visit Insider Pro's Twitter page.

ISTOCK / GETTY IMAGES PLUS / ELENABS / BAGOTAJ

What that means in practice varies widely. One IIoT system could be as simple as a connected rat trap that texts home to say that it's been activated, while another might be as complicated as a fully automated mass-production line that tracks maintenance, productivity and even ordering and shipping information across a huge, multilayered network.

Industrial IoT vs. IoT

The industrial internet of things has also been referred to as the industrial internet (a term coined by GE) and internet of industrial things. Whatever you call it, IIoT is different from other IoT applications in that it focuses on connecting machines and devices in industries such as oil and gas, power utilities and healthcare.

IoT includes consumer-level devices such as fitness bands or smart appliances and other applications that don't typically create emergency situations if something goes wrong.

Simply stated, there is more at stake with IIoT deployments, where system failures and downtime can result in life-threatening or high-risk situations.

IIoT brings computers from IT to operational technology, opening up vast possibilities for instrumentation, leading to major efficiency and productivity gains for almost any industrial operation.

What makes IIoT unique?

Technologically, IIoT works on similar principals as any other piece of IoT tech – automated instrumentation and reporting being applied to stuff that didn't have those capabilities before. That said, the scale of it is much different than a simple system that lets you mess with your thermostat from your phone — hundreds, perhaps thousands or even tens and hundreds of thousands of individual endpoints can be present in an IIoT deployment.

IIoT applications

Instrumentation for production lines can let companies track and analyze their processes on an enormously granular level, asset tracking can give a quick, accessible overview of huge amounts of material, and predictive maintenance can save companies big money by addressing problems before they have a chance to become serious — the number of potential use cases is vast, and growing by the day.

IIoT challenges

IIoT devices can have much longer service lives than consumer gadgetry. The average lifespan of an IIoT device is seven to 10 years, estimates Mike Bell, executive vice president of IoT and devices at Canonical, the company behind Ubuntu Linux. Therefore, IIoT implementations have to be built to last.

Even beyond the raw scale and longevity involved, the implementation process can be convoluted — the kind of back end necessary to make the most of data gleaned from instrumentation is a considerable undertaking in and of itself, and has to be undertaken in close coordination with

THE INDUSTRIAL IoT CONSORTIUM LISTS THESE 15 POSSIBLE USES OF IIoT:

1. Smart factory warehousing applications
2. Predictive and remote maintenance
3. Freight, goods and transportation monitoring
4. Connected logistics
5. Smart metering and smart grid
6. Smart city applications
7. Smart farming and livestock monitoring
8. Industrial security systems
9. Energy consumption optimization
10. Industrial heating, ventilation and air conditioning
11. Manufacturing equipment monitoring
12. Asset tracking and smart logistics
13. Ozone, gas and temperature monitoring in industrial environments
14. Safety and health (conditions) monitoring of workers
15. Asset performance management

the rest of the enterprise. It requires a dedicated strategy for collecting data from endpoints, storing it in an accessible format — whether in a data center or in the cloud — feeding it to the analysis engine, and having a way to turn insights from that analysis into actionable and timely information.

There's a wide range of different formats and technologies that address different parts of the need for machine-to-machine communication among connected devices. Physical layer technology like Sigfox and Zigbee, software layers like Weave and IoTivity — all of it is necessary for a fully functioning IIoT environment, and it all has to be interoperable.

IIoT security concerns

Just like consumer IoT, IIoT has a lot of security issues — remember the Mirai botnet, which leveraged poorly secured security cameras and other gadgets into a huge DDoS weapon.

Beyond the possible use of compromised IIoT devices to create massive botnets, there's also the issue that vulnerabilities can be exploited to allow theft of valuable data already on your network — yet another attack vector.

One thing that might help keep IIoT secure, according to Bell, would be to borrow the increasingly common practice of automatic, silent downloading and patching from the consumer side of IoT. Some companies won't like this, preferring to have absolute control over the software running on their machines, but it could be a big help from a security perspective. ■

JON GOLD *covers IoT and wireless networking for Network World.*

FACTORS THAT IT LEADERS ARE CONCERNED ABOUT INCLUDE THE FOLLOWING:

LACK OF STANDARDIZATION. As an attempt to graft newer technology onto old, there's a huge range of different designs and standards for everything from transmission protocols to ingestion formats. Simply put, if the gizmo that sends operational information about the temperature of a blast furnace isn't made by the same company that makes the network or the data ingestion engine, they might not work together.

INTEGRATION WITH LEGACY TECHNOLOGY. Lots of older equipment isn't designed to provide data in a format that's legible for modern IIoT tech, so getting a decades-old power station controller to talk to a sophisticated new IIoT infrastructure could require some translation.

MONEY. As both of the above points highlight, fully embracing IIoT requires new hardware, new software and a new way of thinking about technology. The idea is to make money, but plenty of people are understandably worried by the up-front costs.

PEOPLE. Getting the most out of IIoT often requires expertise in machine learning, real-time analytics, and data science — to say nothing of cutting-edge knowledge of networking technology.

One thing that might **help keep IIoT secure**, would be to **borrow the increasingly common practice of automatic**, silent downloading and patching from the consumer side of IoT.

YOU'RE PROBABLY DOING YOUR **IIoT IMPLEMENTATION WRONG**

When designing networks and deploying gear for the Industrial industrial of things, **it's important to bring in members of operational technology teams**, not just information technology staff, to make sure business goals of the implementation are met.

BY JON GOLD

THE INDUSTRIAL INTERNET OF THINGS PROMISES a quantum leap forward in automation, centralized management and a wealth of new data and insight that is often too tempting to pass up. But automating a factory floor or a fleet of vehicles is far from simple, and many would-be IIoT adopters are going about the process all wrong, according to experts.

To make an IIoT transition a success, the process has to be led by the line-of-business side of the company — not IT. Successful IIoT adopters frame the entire operation as a matter of digital transformation, aimed at addressing specific business problems, rather than as a fun challenge for IT architects to solve.

Robert Golightly is a senior product marketing manager for Aspen Technology, and he describes himself as a 40-year manufacturing veteran with "a healthy and wholesome disrespect for IT," which, he says, too frequently has an insufficient understanding of how a given company's line of business actually operates.

"This ought to be driven by an expected business outcome," he said. "Rather than just laying claims that 'I've now connected all my assets' or those kinds of things. What business transformation did you really achieve?"

This issue is essentially universal — whether the company in question is trying to leverage IIoT to address supply chain issues, operational excellence or any other business problem, and regardless of the industry in which it operates.

"I think we're guilty of asking ourselves an incomplete set of questions," said Golightly. "We're asking the right questions about how we connect A to B, but I think that the

ISTOCK / GETTY IMAGES PLUS / ELENABS

question we're missing is that, in this new world where we've torn down the silos and we have better information, does it really change the way we make decisions?"

IIoT projects need operational technology pros, not just information technology pros

According to 451 Research IoT practice director Christian Renaud, approaching IIoT from the operational side — via what he calls "the OT door" as opposed to the IT door — is a much more intelligent way to think about implementation.

If an IT person has a wall full of CCNAs in his or her office, it's a safe bet that that person is a member of the Cisco tribe, for example. But OT experts will have certifications of their own. The only way for IT types to get in that door, according to Renaud, is partnership with the OT companies that already know how to make it inside.

"They're absolutely going about IIoT all wrong ... because they're coming through their traditional IT channels," he said. "Honestly, when you look at our survey data about who's actually in charge of that purchasing decision, it's the CEO, the CFO, and maybe one more line-of-business guy that's a digital transformation guy. You know where the CIO is? He's over there at the kids' table eating chicken McNuggets."

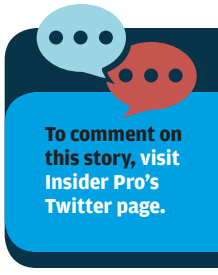
The specificity of the requirements for an IIoT project means that the operational side of the business will generally have a far better idea of what's needed than the IT side.

"An IT and an OT guy walk into a restaurant, and the IT guy goes, 'I'd like a cow and a knife and a match.' And the OT guy goes, 'I'd like a steak,'" said Renaud.

The security risks of doing IIoT wrong

One of the great misconceptions about IIoT is that it's a brand-new concept. Factory floors and utility stations and other major infrastructure have all been automated to one degree or another for decades. What's different, however, is the newly interconnected nature of this technology.

Steve Hanna, senior principal at Infineon Technologies, said that the security risks of IIoT have grown rapidly of late, thanks to a growing awareness of IIoT attack vectors. A factory that was never designed to be connected via the IIoT, with plenty of sensitive legacy equipment that can be 30 years old or older and designed to work via serial cable, can find itself suddenly exposed to the full broadside of remote bad actors, from Anonymous to national governments.



"There's a tool called Shodan that allows you to scan the industrial internet of things for connected industrial equipment, and you'd be surprised at the number of positive results that are found with that tool, things like dams and water and sewer systems," he said.

The most common oversights, according to Hanna, are a lack of two-factor identification, allowing hackers to compromise equipment they find via things like Shodan, and direct interconnections between an operational equipment network and the IIoT.

"We saw that, for example, in the Target attacks of 2009 – they came in through the HVAC system. The HVAC contractor had installed a cellular modem so that they could remotely log in and they wouldn't have to roll a truck in the middle of the night if there was a problem with the HVAC." ■

> Honestly, when you look at our survey data about **who's actually in charge of that purchasing decision**, it's the CEO, the CFO, and maybe one more line-of-business guy that's a digital transformation guy.
>
> CHRISTIAN RENAUD, 451 RESEARCH IOT PRACTICE DIRECTOR

JON GOLD *covers IoT and wireless networking for Network World.*

AN INSIDE LOOK AT AN IIoT-POWERED SMART FACTORY

Despite housing some 50 robots and 50 people, Tempo Automation's gleaming connected factory **RELIES ON INDUSTRIAL IoT AND LOOKS MORE LIKE A HIGH-TECH STARTUP OFFICE THAN A MANUFACTURING PLANT.** BY FREDRIC PAUL

AS SOMEONE WHO'S SPENT HIS WHOLE CAREER working in offices, not factories, I had very little idea what a modern "smart factory" powered by the industrial internet of things (IIoT) might look like. That's why I was so interested in Tempo Automation's new 42,000-square-foot facility in San Francisco's trendy Design District.

Frankly, I pictured the company's facility, which uses IIoT to automatically configure, operate, and monitor the prototyping and low-volume production of printed circuit board assemblies (PCBAs), as a cacophony of robots and conveyor belts attended to by a grizzled band of grease-stained technicians. You know, a 21stcentury update of Charlie Chaplin's 1936 classic *Modern Times* making equipment for customers in the aerospace, medtech, industrial automation, consumer electronics, and automotive industries. (The company has inked a contract with Lockheed Martin.)

Not exactly. Despite housing some 50 robots and 50 people, this gleaming "connected factory" looks more like a high-tech startup office, with just as many computers and few more hard-to-identify machines, including Solder Jet and Stencil Printers, zone reflow ovens, 3D X-ray devices and many more.

How Tempo Automation's 'smart factory' works

On the front end, Tempo's customers upload CAD files with their board designs and Bills of Materials (BOM) listing the required parts to be used. After performing feature extraction on the design and developing a virtual model of the finished product, the Tempo system,

ISTOCK / GETTY IMAGES PLUS / PHONLAMAIPHOTO

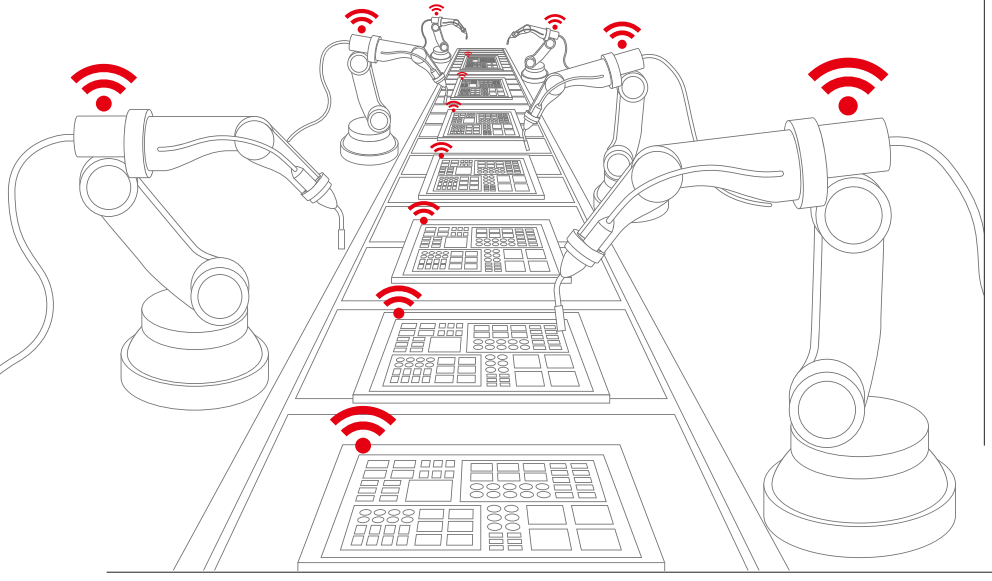
the platform (called Tempocom) creates a manufacturing plan and automatically programs the factory's machines. Tempocom also creates work plans for the factory employees, uploading them to the networked IIoT mobile devices they all carry. Updated in real time based on design and process changes, this "digital traveler" tells workers where to go and what to work on next.

While Tempocom is planning and organizing the internal work of production, the system is also connected to supplier databases, seeking and ordering the parts that will be used in assembly, optimizing for speed of delivery to the Tempo factory.

Connecting the digital thread

"There could be up to 20 robots, 400 unique parts, and 25 people working on the factory floor to produce one order start to finish in a matter of hours," explained Shashank Samala, Tempo's co-founder and vice president of product, in an email. Tempo "employs IIoT to automatically configure, operate, and monitor" the entire process, coordinated by a "connected manufacturing system" that creates an "unbroken digital thread from design intent of the engineer captured on the website, to suppliers distributed across the country, to robots and people on the factory floor."

> There could be up to **20 robots**, **400 unique parts**, and **25 people working on the factory floor** to produce one order start to finish in a matter of hours.
>
> **SHASHANK SAMALA,** CO-FOUNDER AND VICE PRESIDENT OF PRODUCT, TEMPO



ISTOCK / GETTY IMAGES PLUS / METAMORWORKS

Rather than the machines on the floor functioning as "isolated islands of technology," Samala added, Tempo Automation uses Amazon Web Services (AWS) GovCloud to network everything in a bi-directional feedback loop.

"After customers upload their design to the Tempo platform, our software extracts the design features and then streams relevant data down to all the devices, processes, and robots on the factory floor," he said. "This loop then works the other way: As the robots build the products, they collect data and feedback about the design during production. This data is then streamed back through the Tempo secure cloud architecture to the customer as a 'Production Forensics' report."

To comment on this story, visit Insider Pro's Twitter page.

Samala claimed the system has "streamlined operations, improved collaboration, and simplified remote management and control."

Traditional IoT, too

Of course, the Tempo factory isn't all fancy, cutting-edge IIoT implementations. According to Ryan Saul, vice president of manufacturing, the plant also includes an array of IoT sensors that track temperature, humidity, equipment status, job progress, reported defects, and so on to help engineers and executives understand how the facility is operating. ■

FREDRIC PAUL *is editor in chief for New Relic and has held senior editorial positions at ReadWrite, InformationWeek, CNET, PCWorld and other publications.*

WHAT IS A DIGITAL TWIN?

[And how it's changing IIoT, AI and more]

DIGITAL TWINS ARE VIRTUAL REPLICAS OF PHYSICAL DEVICES that data scientists and IT pros can use to run simulations before actual devices are built and deployed. They are also changing how technologies such as IoT, AI and analytics are optimized.

BY KEITH SHAW AND JOSH FRUHLINGER

AS DIGITAL TWIN TECHNOLOGY plays an increasingly important role in the industrial internet of things (IIoT), it is also moving beyond basic manufacturing applications.

More complex "things" are becoming connected with the ability to produce data, so having a digital equivalent gives data scientists and other IT professionals the ability to optimize deployments for peak efficiency and create other what-if scenarios.

What is a digital twin?

A digital twin is a digital representation of a physical object or system. The technology behind digital twins has expanded to include large items such as buildings, factories and even cities, and some have said people and processes can have digital twins, expanding the concept even further. The idea first arose at NASA: full-scale mockups of early space capsules, used on the ground to mirror and diagnose problems in orbit, eventually gave way to fully digital simulations.

But the term really took off after Gartner named digital twins as one of its top 10 strategic technology trends for 2017 saying that within three to five years, "billions of things will be represented by digital twins, a dynamic software model of a physical thing or system". A year later, Gartner once again named digital twins as a top trend, saying that "with an estimated 21 billion connected sensors and endpoints by 2020, digital twins will exist for billions of things in the near future."

In essence, a digital twin is a computer program that takes real-world data about a physical object or system as inputs and produces as outputs predications or simulations of how that physical object or system will be affected by those inputs.

How does a digital twin work?

A digital twin begins its life being built by specialists, often experts in data science or applied mathematics. These developers research the physics that underlie the physical object or system being mimicked and use that data to develop a mathematical model that simulates the real-

ISTOCK / GETTY IMAGES PLUS / JUST_SUPER

world original in digital space.

The twin is constructed so that it can receive input from sensors gathering data from a real-world counterpart. This allows the twin to simulate the physical object in real time, in the process offering insights into performance and potential problems. The twin could also be designed based on a prototype of its physical counterpart, in which case the twin can provide feedback as the product is refined; a twin could even serve as a prototype itself before any physical version is built.

The process is outlined in some detail in this post from Eniram, a company that creates digital twins of the massive container ships that carry much of world commerce — an extremely complex kind of digital twin application. However, a digital twin can be as complicated or as simple as you like, and the amount of data you use to build and update it will determine how precisely you're simulating a physical object. For instance, this tutorial outlines how to build a simple digital twin of a car, taking just a few input variables to compute mileage.

Digital twins and IoT

Clearly, the explosion of IoT sensors, initially in industry and now in consumer products, are part of what makes digital twins possible. And as IoT devices are refined, digital-twin scenarios can include smaller and less complex objects, giving additional benefits to companies.

Digital twins can be used to predict different outcomes based on variable data. This is similar to the run-the-simulation scenario often seen in science-fiction films, where a possible scenario is proven within the digital environment. With additional software and data analytics, digital twins can often optimize an IoT deployment for maximum efficiency, as well as help designers figure out where things should go or how they operate before they are physically deployed.

The more that a digital twin can duplicate the physical object, the more likely that efficiencies and other benefits can be found. For instance, in IIoT, where the more highly instrumented devices are, the more accurately digital twins might simulate how the devices have performed over time, which could help in predicting future performance and possible failure.

Digital-twin vendors

Building a digital twin is complex, and there is as yet no standardized platform for doing so. Ian Skerrett, a consultant working in the field who has long history in open source behind him, has proposed the outline of a digital twin platform, though this is a first step, as suits the rather embryonic nature of the space.

In contrast with many emerging

DIGITAL-TWIN USE CASES

These two digital-twin examples — the car and the cargo vessel — give you a sense of potential use cases. Objects such as aircraft engines, trains, offshore platforms and turbines can be designed and tested digitally before being physically produced. These digital twins could also be used to help with maintenance operations. For example, technicians could use a digital twin to test that a proposed fix for a piece of equipment works before applying the fix the physical twin.

Digital-twin business applications are found in a number of sectors:

MANUFACTURING is the area where rollouts of digital twins are probably the furthest along, with factories already using digital twins to simulate their processes, as this case study from Deloitte

AUTOMOTIVE digital twins are made possible because cars are already fitted with telemetry sensors, but refining the technology will become more important as more autonomous vehicles hit the road.

HEALTHCARE is the sector that produces the digital twins of people we mentioned above. Band-aid sized sensors send health information back to a digital twin used to monitor and predict a patient's well-being.

technologies, commercial digital-twin offerings are actually coming from some of the largest companies in the field. For instance, GE, which developed digital-twin technology internally as part of its jet-engine manufacturing process, is now offering its expertise to customers, as is Siemens, another industrial giant heavily involved in manufacturing. Not to be outdone by these factory-floor suppliers, IBM is marketing digital twins as part of its IoT push, and Microsoft is offering its own digital-twin platform under the Azure umbrella.

Digital twin vs. predictive twin

In an article for Network World, contributor Deepak Puri outlined an example of an Oracle digital-twin tool that provides users with two options — a digital twin and a predictive twin.

The digital twin "can include a description of the devices, a 3D rendering and details on all the sensors in the device. It continuously generates sensor readings that simulate real life options."

The predictive twin "models the future state and behavior of the device," Puri writes. "This is based on historical data from other devices, which can simulate breakdowns and other situations that need attention."

As part of its digital-twin initiative Microsoft is taking the concept and applying it to processes in addition to physical products. In a whitepaper, Microsoft proposes the idea of the digital process twin:

"The Process Digital Twin is the next level of digital transformation, compounding Product Digital Twin benefits throughout the factory and supply chain," Microsoft states. The associated whitepaper highlights some advanced manufacturing scenarios that product digital twins don't support, but that process digital twins would.

Benefits of digital twins

Digital twins offer a real-time look at what's happening with physical assets, which can radically alleviate maintenance burdens. Chevron is rolling out digital twin tech for its oil fields and refineries and expects to save millions of dollars in maintenance costs. And Siemens as part of its pitch says that using digital twins to model and prototype objects that have not been manufactured yet can reduce product defects and shorten time to market.

But keep in mind that that Gartner warns that digital twins aren't always called for, and can unnecessarily increase complexity. "[Digital twins] could be technology overkill for a particular business problem. There are also concerns about cost, security, privacy, and integration."

Digital-twin skills

Interested in becoming a digital twin pro? The skill sets are demanding, and require specialized expertise in machine learning, artificial intelligence, predictive analytics and other data-science capabilities. That's part of the reason why big companies are hanging out their shingle in this space: the little guy might find it more reasonable to hire a consultant team than to upskill their in-house workers. ■

OTHER DIGITAL-TWIN RESOURCES

Microsoft — Digital Twins in Discrete Manufacturing

GE — Predix Digital Twin site

GE — Digital Twin at Work: The Technology that's Changing Industry

IBM — Industry Transformation with IBM Digital Twin (PDF)

Siemens — Digitization in machine building

Oracle — Digital Twins for IoT Applications (PDF)

KEITH SHAW *is former Network World editor. He is now a freelance writer and editor based in Worcester, Mass.*

JOSH FRUHLINGER *is a writer and editor who lives in Los Angeles.*

ISTOCK / GETTY IMAGES PLUS / OSTAPENKOOLENA

INSIDER EXCLUSIVE

To securely build and grow an IoT ecosystem, **enterprises must have the tools and architectures in place to identify, control and manage their IoT devices.** This has especially important implications for industrial IoT. **BY NISARG DESAI**

IDENTIFYING IoT — ONE DEVICE AT A TIME

AS IoT MOVEMENT PERVADES EVERY FACET OF OUR LIVES, the pace of innovation in this field continues to grow. However, this being a classic case of trying to run before we've learned how to walk, IoT device developers often leave out the core component of any connected service in today's world — security. This has a particularly crucial impact on industrial IoT.

There are very few standards in place for IoT security — cyber or physical. Hence, a lot of IT standards are being modified or drawn upon to come up with reference architectures and security best practices for IoT security. Common among these frameworks is the need for a strong, unique and immutable identity for each IoT device. While there are various ways to establish this, industry analysts, major cloud platform providers, thought leaders and early adopters all agree that Public Key Infrastructure (PKI) is going to be the chosen mechanism for this, now and into the future. PKI itself has had to adapt and is now moving into the 21st century with increased adoption, but also widespread application to a varied number of use-cases.

Core to a PKI-based infrastructure is a trusted third-party, a Certificate Authority (CA). CAs have existed for decades and today issue publicly (or privately) trusted credentials entities that need to prove their identity. As such, a digital certificate issued by CAs is a universally accepted identity credential on most digital platforms.

An important component or function of a CA is the act of 'registration' commonly performed by the Registration Authority (RA). The RA sits between the entity that is requesting an identity and the CA and essentially implements a layer of control and management over the verification of identity prior to issuance. It

ISTOCK / GETTY IMAGES PLUS / WENJIE DONG / FLEAZ

is responsible for checking that a particular public key belongs to the entity requesting a certificate for it.

Building a registration authority for the IoT

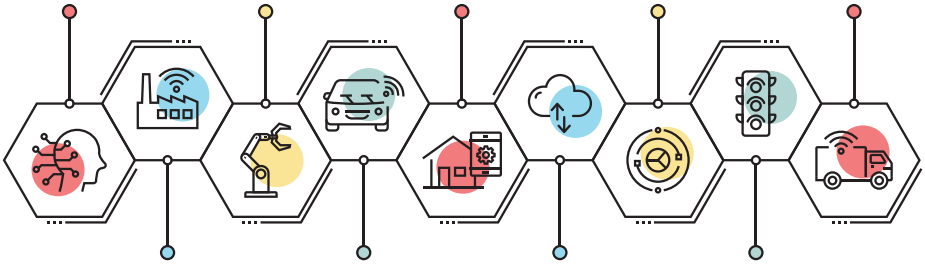
So how do we build a Registration Authority for the IoT?

First, we need to think of ways we can offer policy-based control to end-users who can define how exactly a device needs to behave for it to be considered an authentic device. Secondly, we need to apply this to a large common set of devices — this problem is exacerbated by the different provisioning environments that a device can be used in. We need to account for both greenfield enrollment (devices that are new or still being manufactured) as well as brownfield enrollment (devices that have already been deployed and are in use). Finally, we need to add ancillary layers like a configuration and rules engine, grouping and classification of devices, etc. This would create a Local Registration Authority or LRA and we could have deployment environment specific LRAs.

What could we use to define the authenticity of a device?

1. A PRE-EMBEDDED ROOT OF TRUST (ROT)

Many IoT and IIoT devices come with a pre-embedded identifier that was injected during manufacturing in a secure process. This could be a simply pre-shared secret like a key, a unique serial number, or another certificate, sometimes called a birth certificate. We could also use a hardware secure element embedded in the device — a Trusted Platform Module (TPM) or hardware based Physically Unclonable Function (PUF).



2. A DEVICE WHITELIST

We can upload a list of common identifiers, example a MAC address and thus create a whitelist of allowable devices which is then uploaded to the RA. The RA would then do a pre-issuance check against this whitelist.

3. CHALLENGE-RESPONSE

The RA could perform a challenge response check on the IoT device. For instance, the device would produce a public key. If this public key is on a pre-approved whitelist, the RA would then challenge the device to prove possession of the associated private key. A successful check would result in the device getting enrolled and being issued a certificate.

4. BEHAVIORAL SIGNATURE

For IoT devices where we do not have a pre-embedded ROT, we could rely on less secure methods for verifying authenticity. For instance, we could use the behavioral characteristics of the device to determine and identify a specific or a class of devices. One method is to generate a hash of selected files in the files system and compare that to pre-computed hashes from a golden image — a sort of device fingerprinting.

5. ENVIRONMENTAL CHECKS

If we have even fewer options to rely upon for verifying authenticity, we could rely upon specific environmental characteristics within which a device is deployed. For instance, we could use a combination of the IP address to locate the geographic source of an incoming request (to the RA) and combine this with a time-window during which devices are likely to connect based on pre-programmed schedules. While not completely secure, this is more of a good-enough approach.

6. ONE-TIME TRUST EVENT

Finally, we can perform a one-time trust event — basically we assume a device to be true and authentic once, to be able to perform a device enrollment and provision it with an initial device identifier or ROT. The closer this is done to the manufacturing stage, or earlier in the supply chain, the better it is. However, this can also be done for devices that are guaranteed to be deployed in a secure environment. To mitigate risks, we can even provision a temporary or one-time use key that cannot be used if the device leaves and returns to that environment and/or system.

As you can see we've provided a number of options that can be used

to construct your own device RA service and the policies that can be configured to accept or reject a device as authentic. Each type of verification is different and usually a combination of several factors must be used to guarantee that a device is who it claims to be. Also, once registration is performed, depending upon the credential's validity or ecosystem policy we may need to perform registration on a periodic basis.

Older IT standards like IEEE 802.1AR specify long-lived device certificates called Initial Device Identifiers (IDevID) that essentially never expire, are being adapted and adopted for Industrial Internet of Things (IIoT). Again, these are simply birth certificates and can only be used for identity verification. These are then used to bootstrap into more deployment ecosystem specific credentials called the Locally Significant Device Identifier (LDevID) that can be used for authentication, authorization, secure communications, etc. LDevID certificates are typically shorter lived.

Implications for the IIoT

IIoT has very specific challenges that a Device RA (DRA) or IoT-specific RA can help solve.

First, the sheer breadth of use-cases and physical environments that an IIoT system is deployed in makes it very challenging to have a universal identity mechanism for all of your connected devices.

Secondly, there are machines that have existed for many years, and will continue to function for decades more — and we then introduce newer devices into this ecosystem that are very different than their older counterparts.

This mash up of greenfield and brownfield devices mandates that we cannot have a completely new, rip-and-replace approach. We need to build systems and solutions that work with existing technology and management platforms and provide options to gracefully on board these older devices onto newer IoT platforms. Finally, we need to meld the IT and OT systems into one. Since IT is already very familiar with PKI based identities, this isn't a problem on their side. However, we need to educate and create enough context and value around said solution so that it caters to OT users and persons as well.

As an example, let's take a look at the Smart Electric Grid, and some of the work being done by the Wireless Smart Ubiquitous Networks (Wi-SUN) Alliance and their Field Area Network (FAN) specification. This is a wireless mesh network architecture that allows Smart Meters to talk independently to each other, as well as to head-end controllers (put simply). This leads to more resilient and highly available network that can dynamically route traffic in the case of any failures to critical nodes. Newer devices can automatically enter and exit a given network. This happens completely autonomously.

Hence, it is extremely important here for devices to be able to talk with each other directly and authenticate one another without the need of a third party. A local, device specific RA service is the best solution for such a scenario.

As you can see, PKI is evolving, and we are now applying some of the core tenets of cybersecurity that are part of PKI, to IoT use-cases. Remember, there is no need to re-invent the wheel — in this case, simply to develop new ways of using it. The Internet of Things is still the internet — the same security principles that have safeguarded networks for decades will continue to do protect this 'new' internet. We simply must be cyber-aware and implement security from the get-go. ■

NISARG DESAI *is a software engineer with experience in product management and leadership spanning the information and cybersecurity, hospitality services, and business consulting industries. He is director of product management, IoT, at GlobalSign.*

We need to build systems and solutions that work with **existing technology** and management platforms and provide **options** to gracefully on board these older devices onto **newer IoT platforms**.